UNITED STATES DISTRICT COURT

FOR THE MIDDLE DISTRICT OF FLORIDA

MELODY T. BRANTLEY, Plaintiff, v. ZEROED-IN TECHNOLOGIES, LLC and DOLLAR TREE, INC., Defendants.	**Case No:** **CLASS ACTION COMPLAINT** JURY TRIAL DEMAND

AMENDED CLASS ACTION COMPLAINT

SUMMARY OF THE CLASS ACTION

Plaintiff Melody T. Brantley ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her undersigned attorneys, brings this class action against Zeroed-In Technologies, LLC ("Zeroed-In") and Dollar Tree, Inc. ("Dollar Tree") (collectively, "Defendants") and complains and alleges upon personal knowledge as to herself and upon information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard the personally identifiable information of approximately 1.977 million individuals, including employees and clients of Zeroed-In's client, Dollar Tree, which owns the Dollar Tree and Family Dollar chain of retail stores.

2. Defendant Zeroed-In, a Fort-Myers, Florida-based data company, provides a cloud-based human resource ("HR") analytics platform for businesses. The software it provides help

collect, analyze, and visualize workforce data. In the ordinary course of doing business with Zeroed-In or seeking employment through one of its many clients, individuals are required to provide and entrust Zeroed-In with sensitive Personally Identifiable Information ("PII"). Upon information and belief, Defendant Dollar Tree is one of Zeroed-In's clients and required their employees to entrust them with sensitive, non-public PII as a condition of employment, which Dollar Tree retails electronically.

3. On November 27, 2023, Zeroed-In reported a data security incident with the Office of the

Maine Attorney General and, on the same day, began sending out data breach letters to individuals whose information was compromised because of the data security incident (the "Notice").[1]

4. Zeroed-In reported that, on or around August 8, 2023, Zeroed-In detected unusual activity on certain of its computer network systems occurring between August 7, 2023, and August 8, 2023, and responded by launching an internal investigation into the suspicious activity. Zeroed-In's investigation revealed that one or more unauthorized individuals breached Zeroed-In's network and gained access to certain files containing the sensitive information of employees and clients of Dollar Tree.[2]

5. Zeroed-In admitted that the impacted files contained sensitive PII, including the "names, dates of birth, and/or Social Security number[s]" of approximately 1.977 million individuals.[3]

[1] *Notice of Data Event*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/b3993ddd-2443-4645-ae45-f36dc7686236.shtml (last accessed December 8, 2023).
[2] *Id.*
[3] *Id.*

6. Zeroed-In provided limited details about the Data Breach, including whether the cybercriminal(s) responsible for breach were identified or whether the information exfiltrated was held for ransom. Zeroed-In also failed to disclose whether its investigation detected the compromised information on the dark web. Instead, Zeroed-In stated that "as part of our ongoing to commitment to the security of your information, we are reviewing our existing policies and procedures and implemented additional safeguards to prevent a similar event from occurring in the future."[4] Zeroed-In also offered access to Single Bureau Credit Monitoring at no charge to affected individuals, but as Plaintiff's allegations will make clear, this offer is woefully inadequate.[5]

7. Despite learning of the Data Breach as early as August 8, 2023, Zeroed-In failed to announce the Data Breach publicly until almost four months later on or around November 27, 2023, and did not begin sending out Data Breach notification letters to affected individuals until around that time.

8. Zeroed-In's Notice failed to disclose how it discovered the encrypted files on its computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the delay in notifying Plaintiff and the class of the Data Breach, how Zeroed-In determined that the PII had been "accessed" by an unauthorized party, and importantly, what specific steps Zeroed-In took following the Data Breach to secure its systems and prevent future cyberattacks.

9. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII from the foreseeable threat of a cyberattack.

[4] *Id.*
[5] *Id.*

10. By being entrusted with Plaintiff's and class members' PII for their own pecuniary benefit, Defendants assumed a duty to Plaintiff and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and class members' PII against unauthorized access and disclosure. Defendants also had a duty to adequately safeguard this PII under controlling Florida case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "FTC Act"). Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII in their possession from unauthorized access and disclosure.

11. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff and approximately 1.977 million class members suffered injury and ascertainable losses in the form of out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from their exposure, and the present and imminent threat of fraud and identity theft. This action seeks to remedy these failings and their consequences.

12. The injury to Plaintiff and class members was compounded by the fact that Defendants did not notify those affected that their PII was subject to unauthorized access and exfiltration until November 2023, nearly four months after the Data Breach was discovered. Defendants' failure to timely notify the victims of their Data Breach meant that Plaintiff and class members were unable to immediately take affirmative measures to prevent or mitigate the resulting harm.

13. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and class members' sensitive and confidential PII remains in the possession of Defendants. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft.

14. Defendants disregarded the rights of Plaintiff and class members by, *inter alia*, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train their staff and employees on proper security measures; and failing to provide Plaintiff and class members prompt and adequate notice of the Data Breach.

15. In addition, Defendants failed to properly monitor the computer network and systems that housed the PII. Had Defendants properly monitored these electronic systems, they would have discovered the intrusion sooner or prevented it altogether.

16. The security of Plaintiff's and class members' identities is now at risk because of Defendants' wrongful conduct as the PII that Defendants collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

17. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes including, for example, opening new financial accounts in class members' names, taking out loans in their names, using class members' identities to obtain government benefits, filing fraudulent tax returns using their information, obtaining driver's licenses in class members' names, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and class members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and class members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and class members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

19. Plaintiff and class members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. And because the exposed information includes Social Security numbers and other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

20. Plaintiff brings this action on behalf of herself and individuals in the United States whose Personal Information was exposed because of the Data Breach, Defendants learned of on or about August 8, 2023, and first publicly acknowledged on or about November 23, 2023. Plaintiff and class members seek to hold Defendants responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information. Plaintiff seeks to remedy the harms resulting from the Data Breach on behalf of herself and all similarly situated individuals whose Personal Information was accessed and exfiltrated during the Data Breach.

21. Plaintiff, on behalf of herself and all other class members, brings claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiff and class members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training

practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

Plaintiff

22. Plaintiff Melody T. Brantley is a citizen of Texas and resides in Marshall, Texas. Plaintiff provided her PII to Zeroed-In, or otherwise had her PII provided to Zeroed-In, in connection with her employment at Family Dollar. In receiving and maintain her PII for its business purposes, Zeroed-In expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's PII. Zeroed-In, however, did not take proper care of Plaintiff's PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Zeroed-In's inadequate security measures.

23. Plaintiff has suffered harm because of the Data Breach. Since learning of the Data Breach, Plaintiff has spent more than 15 hours researching the potential consequences of the Data Breach and checking her credit and financial accounts for unauthorized activity, which are practices Plaintiff will need to continue to indefinitely conduct to protect herself against fraud and identity theft.

24. Plaintiff has been made aware by credit reporting bureaus, including Experian, that her PII is now on the Dark Web. Consequently, she took it upon herself to lock her credit account with Experian due to the risk that more of her information will be released onto the Dark Web.

25. Plaintiff also suffered actual injury from having her PII compromised because of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of her confidential personal information—a form of property that Plaintiff entrusted to Defendants,

which was compromised because of the Data Breach it failed to prevent and (b) a violation of her privacy rights because of Defendants' unauthorized disclosure of her PII.

26. Had Plaintiff known that Defendants do not adequately protect PII, she would not have agreed to provide Defendants with her PII or agreed to have her PII provided to Defendants.

27. As a result of Defendants' failure to adequately safeguard Plaintiff's information, she has been injured. Plaintiff is also at a continued risk of harm because her information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendants fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

Defendants

28. Defendant Zeroed-In is a limited liability company organized under the laws of the State of Florida. Zeroed-In maintains its principal place of business at 11037 Harbor Yacht Ct., #201, Fort Myers, Florida 33908, with its mailing address at 8595 College Parkway, Suite 350, Fort Myers, Florida 33919.

29. Zeroed-In operates a cloud-based HR analytics business that helps collect, analyze, and visualize workface data. According to the company's website, it has over 70 clients, 30,000 registered users, and approximately 2.7 million "work lives."[6]

30. Defendant Dollar Tree is a company incorporated under the laws of Virginia, with its principal place of business located at 500 Volvo Parkway, Chesapeake, Virginia 23320. Defendant Dollar Tree was a client of Defendant's Zeroed-In's human resources data

[6] Ernestas Naprys, Almost Two Million Affected by Data Company Zeroed-In Technologies Breach, CYBERNEWS (November 28, 2023), accessible at: https://cybernews.com/security/almost-two-million-affected-zeroedin-technologies-breach/ (last accessed December 8, 2023).

analytics products.[7] Additionally, Defendant Dollar Tree shares human resources PII with Defendant Zeroed-In, a third-party analytics vendor.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Zeroed-In. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

32. This Court has general personal jurisdiction over Zeroed-In because Zeroed-In's principal place of business is in this District. Christopher Moore, who is identified as the CEO and "Manager" of Zeroed-In on Zeroed-In's most recent annual report filed with the Florida Secretary of State on January 18, 2023, also has an address within this District: 11037 Harbor Yacht Ct., #201, Fort Myers, Florida 33908. This Court has specific personal jurisdiction over Dollar Tree in this matter because Dollar Tree availed itself of Zeroed-In's services with respect to Plaintiff's claims.

33. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Zeroed-In has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

A. Overview of Defendants' Businesses

[7] *Dollar Tree hit by third-party data breach impacting 2 million people,* Bleeping Computer, https://www.bleepingcomputer.com/news/security/dollar-tree-hit-by-third-party-data-breach-impacting-2-million-people/#:~:text=Discount%20store%20chain%20Dollar%20Tree,the%20United%20States%20and%20Canada. (last accessed December 8, 2023).

34. Zeroed-In is a data management consulting firm that provides workforce analytics solutions to corporate clients. Zeroed-In specializes in data management, data visualization, and people analytics, all of which serve as Zeroed-In's human resource platform. Put simply, Zeroed-In collects PII contained by its "customers" for hosting and processing purposes in connection with a subscription to [Zeroed-In's] products or services…"[8] Zeroed-In employs more than 2,500 people and generates approximately $5.2 million in annual revenue.[9]

35. In the regular course of its business, Zeroed-In collects and maintains the PII of its corporate clients' employees and other persons as a condition to providing workforce analytics services. Zeroed-In stores this information digitally. Zeroed-In specifies in its Privacy Policy that it uses collected PII "to perform the services requested by the user [,]…for marketing purposes[,]…" and to manage and ameliorate the webpages through which Zeroed-In operates and collects data, facilitate the utilization of such webpages, and "track aggregate traffic patterns throughout" such webpages.[10]

36. Zeroed-In's Privacy Policy ensures its clients and other related persons that it is "committed to protecting the privacy of your information" and that it "employ[s] robust security measures to protect against the loss, misuse and alternation of the personal information under our control."[11]

37. Dollar Tree operates over 8,000 low-price retail stores in the U.S. and Canada, under the Dollar Tree and Family Dollar brands.[12]

---

[8] *Privacy Policy*, Zeroed-In Technologies, http://www.zeroedin.com/privacy-policy/. (last accessed December 8, 2023).
[9] Richard Console, Jr., ZeroedIn Technologies Notifies 1.9 Million Consumers of Data Breach Affecting Their SSNs, JD SUPRA (November 28, 2023), accessible at: https://www.jdsupra.com/legalnews/zeroedin-technologies-notifies-1-9-1390357/. (last accessed December 8, 2023).
[10] *Privacy Policy*, Zeroed-In Technologies, http://www.zeroedin.com/privacy-policy/. . (last accessed December 8, 2023).
[11] *See* https://www.zeroedin.com/privacy-policy/ (last accessed December 8, 2023).
[12] *See* https://corporate.dollartree.com/about/our-brands/dollar-tree (last accessed December 8, 2023).

38. As a condition of employment, Zeroed-In's clients, including Dollar Tree, require their employees and other affiliated persons, including Plaintiff and Class Members, to entrust them with highly sensitive PII.

39. By obtaining, collecting, using, and benefitting from Plaintiff's and class member's PII, Defendants assumed legal and equitable duties to them that required Defendants to, at a minimum, implement adequate safeguards to prevent unauthorized use or disclosure of PII and to report any unauthorized use or disclosure of PII.

40. Plaintiff and Class members are, or were, employees or customers of Defendants, or otherwise, are affiliated or transacted with Defendants and entrusted Defendants with their PII.

41. Plaintiff and Class Members reasonably relied on Defendants to maintain the confidentiality and security of their PII and only to make required, authorized disclosures of this information, which Defendants ultimately failed to do. Compounding Defendants' breach of these duties, Defendants waited approximately four months after discovering the Data Breach to notify those affected that their PII had been compromised.

B. The Data Breach Compromised Plaintiff's and Class Members' PII

42. On or about August 8, 2023, according to the notice Zeroed-In submitted to the Office of the Maine Attorney General, Zeroed-In detected unusual activity on its systems. The notice stated that Zeroed-In "determined that an unauthorized actor gained access to certain systems between August 7, 2023, and August 8, 2023. While the investigation was able to determine that these systems were accessed, it was not able to confirm all of the specific files that were accessed or taken by the unauthorized actor."[13]

[13] *See Notice of Data Event,* n.1, *supra*.

43. Zeroed-In did not publicly announce the Data Breach until on or around November 23, 2023.[14] Zeroed-In admitted that the unauthorized party accessed files within its system that included sensitive PII, including "names, dates of birth, and/or Social Security numbers" used by Zeroed-In for its business operations.[15]

44. Zeroed-In's Notice vaguely describes the measures it took following its discovery of the Data Breach, stating only that it "immediately took steps to secure the systems and launched an investigation into the nature and scope of the activity" and that it "moved quickly to investigate and respond to the incident, access the security of Zeroed-In systems, and identify potentially affected individuals and Zeroed-In customers."[16]

45. Zeroed-In's Notice omits pertinent information including how criminals gained access to the encrypted files on its systems, what computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the delay in notifying Plaintiff and class members of the Data Breach, how it determined that the PII had been accessed, and of particular importance to Plaintiff and class members, what actual steps Zeroed-In took following the Data Breach to secure its systems and train its employees to prevent further cyberattacks.

46. Based on Zeroed-In's acknowledgment that "an unauthorized actor gained access to certain systems" and determined that certain "information was present at the time of the incident," it is evident that unauthorized criminal actors did in fact access Zeroed-In's network and exfiltrate Plaintiff's and class members' PII in an attack designed to acquire that sensitive, confidential, and valuable information.[17]

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*

47. The PII contained in the files accessed by cybercriminals appears not to have been encrypted because if properly encrypted, the attackers would have acquired unintelligible data and would not have "accessed" Plaintiff's and class members' Personal Information.[18]

48. Zeroed-In did not confirm whether some or all its locations were impacted by the Data Breach, but Defendant Dollar Tree was included as one of Defendant Zeroed-In's clients affected by the Data Breach.[19] Overall, the Data Breach reportedly impacted the Zeroed-In of approximately 1.977 million individuals like Plaintiff and class members.

49. As corporate entities that collect, create, and maintain significant volumes of Personal Information, the targeted attack was a foreseeable risk of which Defendants were aware and knew they had a duty to guard against.

50. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of Defendants' employees and other individuals who are affiliated or transacted with Defendants.

51. Despite detecting the Data Breach on or around August 8, 2023, Defendants waited approximately four months to notify the impacted individuals of the Data Breach and of the need for them to protect themselves against fraud and identity theft. Defendants were, of course, too late in the discovery and notification of the Data Breach in contravention of their legal duty to protect such information.

52. Due to Defendants' inadequate security measures and their delayed notice to victims, Plaintiff and class members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

[18] *Id.*
[19] *Id.*

53. Defendants had obligations created by contract, industry standards, Section 5 of FTC Act, and common law made to Plaintiff and class members to keep their PII confidential and to protect it from unauthorized access and disclosure.

54. Plaintiff and class members entrusted their PII to Defendants with the reasonable expectation and mutual understanding that Defendants or anyone who used their PII in conjunction with workface analytics or HR services would comply with obligations to keep such information confidential and secure from unauthorized access after it received such information.

55. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and class members' PII from unauthorized disclosure.

56. Plaintiff and the class members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiff and class members would not have allowed Zeroed-In or anyone in Zeroed-In's position to receive their PII had they known that Zeroed-In would fail to implement industry standard protections for that sensitive information.

57. As a result of Defendants' negligent and wrongful conduct, Plaintiff's and class members' highly confidential and sensitive Personal Information was left exposed to cybercriminals.

C. Defendants Failed to Follow FTC Guidelines

58. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information

is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

59. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

60. According to the FTC< the need for data security should be factored into all business decision-making.

61. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

62. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

63. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

64. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

65. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. Defendants failed to properly implement basic data security practices.

67. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

68. Defendants were at all times fully aware of their obligation to protect the Personal Information of the employees and customers of their clients who entrusted Defendants with their PII. Defendants were also aware of the significant repercussions that would result from their failure to do so.

D. Defendants Failed to Comply with Industry Standards for Data Security

69. Experts studying cyber security routinely identify corporations as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

70. Several best practices have been identified that at a minimum should be implemented by corporate entities like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

71. Other standard best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and

routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

72. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. These foregoing frameworks are existing and applicable industry standards in the corporate industry and Defendants failed to comply with these accepted standards, thereby opening the door to cybercriminals and causing the Data Breach.

E. Defendants Owed Plaintiff and Class Members a Duty to Safeguard Their Personal Information

74. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of class members.

75. Zeroed-In owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including

adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII.

76. Defendants owed a duty to Plaintiff and Class members to implement processes that would detect a compromise of PII in a timely manner.

77. Defendants owed a duty to Plaintiff and Class members to act upon data security warnings and alerts in a timely fashion.

78. Defendants owed a duty to Plaintiff and Class members to disclose in a timely and accurate manner when and how the Data Breach occurred.

79. Defendants owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices.

F. Defendants Knew That Criminals Target PII

80. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

81. At all relevant times, Defendants knew, or should have known, that Plaintiff's, and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

82. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII customers and employees of Defendants' clients, like Plaintiff and class members.

83. Personal Information is a valuable property right.[20] The value of Personal Information as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[23] It is so valuable to identity thieves that once Personal Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web" for many years.

84. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, Personal Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

85. Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[24] Experian reports that a stolen credit or debit card

---

[20] See Marc van Lieshout, The Value of Personal Data, 457 IFIP Advances in Information and Communication Technology (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."). (last accessed December 8, 2023).

[21] See Robert Lowes, Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market, Medscape (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 .(last accessed December 8, 2023).

[22] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, No. 220, p.4, OECD Publishing (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last accessed December 8, 2023)

[23] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, Interactive Advertising Bureau (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last accessed December 8, 2023).

[24] Anita George, Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends (Oct. 16, 2019), accessible at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs// (last accessed December 8, 2023).

number can sell for $5 to $110 on the dark web.[25] All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[26] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[27] According to a report released by the Federal Bureau of Investigation's (FBI) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[28]

86. Criminals can use stolen Personal Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[29] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . .. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[30]

87. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies

[25] Brian Stack, Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian (Dec. 6, 2017), accessible at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed December 8, 2023).
[26] Adam Greenberg, Health insurance credentials fetch high prices in the online black market, SC Magazine (July 16, 2013), accessible at https://www.scmagazine.com/news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last accessed December 8, 2023).
[27] In the Dark, VPNOverview.com, accessible at https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed December 8, 2023).
[28] See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, FBI Cyber Division (Apr. 8, 2014), accessible at https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last accessed December 8, 2023).
[29] Andrew Steger, What Happens to Stolen Healthcare Data? HealthTech (Oct. 30, 2019), accessible at https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last accessed December 8, 2023).
[30] *Id.*

confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[31]

88. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

89. Indeed, cyberattacks have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[32]

90. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[33]

91. Defendants were on notice that the federal government has been concerned about company data encryption practices. Defendants knew their employees accessed and utilized protected consumer information in the regular course of their duties, yet it appears that information was not encrypted.

---

[31] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) Information Systems Research 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1 (last accessed December 8, 2023).

[32] Gordon M. Snow, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, FBI (Sept. 14, 2011), accessible at https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last accessed December 8, 2023).

[33] Ben Kochman, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), accessible at https://www.law360.com/articles/1220974 (last accessed December 8, 2023).

92. The Office for Civil Rights ("OCR") urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[34]

G. Theft of PII Has Grave and Lasting Consequences for Victims

93. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, received medical treatment, start new utility accounts, and incur charges and credit in a person's name.[35]

94. Identity thieves use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[36] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit

[34] Stolen Laptops Lead to Important HIPAA Settlements, U.S. Department of Health and Human Services (Apr. 22, 2014), accessible at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/concentra-health-services/index.html (last accessed December 8, 2023).
[35] See What to Know About Identity Theft, Federal Trade Commission Consumer Advice, accessible at https://www.consumer.ftc.gov/articles/what-know-about-identity-theft(last accessed on December 8, 2023).
[36] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.[37]

95. With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and SSN to obtain government benefits, or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[38]

96. Each year, identity theft causes billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and class members.

97. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on dark web black-markets for years.

---

[37] Susan Henson, What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?, Experian (May 21, 2023), accessible at https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed on December 8, 2023).

[38] See Warning Signs of Identity Theft, Federal Trade Commission, accessible at https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed on December 8, 2023).

98. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

99. The PII exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[39]

100. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

101. [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[40]

102. For instance, with a stolen Social Security number, which is only one subset of the Personal Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[41]

103. Identity thieves can use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the

[39] Ari Lazarus, How fast will identity thieves use stolen info?, Federal Trade Commission (May 24, 2017), accessible at https://www.linkedin.com/pulse/how-fast-identity-thieves-use-stolen-info-brian-allen/ (last accessed on December 8, 2023).

[40] Report to Congressional Requesters: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, United States Government Accountability Office, accessible at https://www.gao.gov/assets/gao-07-737.pdf (last accessed on December 8, 2023).

[41] See, e.g., Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number (Nov. 2, 2017), accessible at https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last accessed on December 8, 2023).

victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

104. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

105. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[42]

106. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

107. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your

[42] 2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends, and Workplaces, Identity Theft Resource Center (2021), accessible at https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last accessed on December 8, 2023).

name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[43]

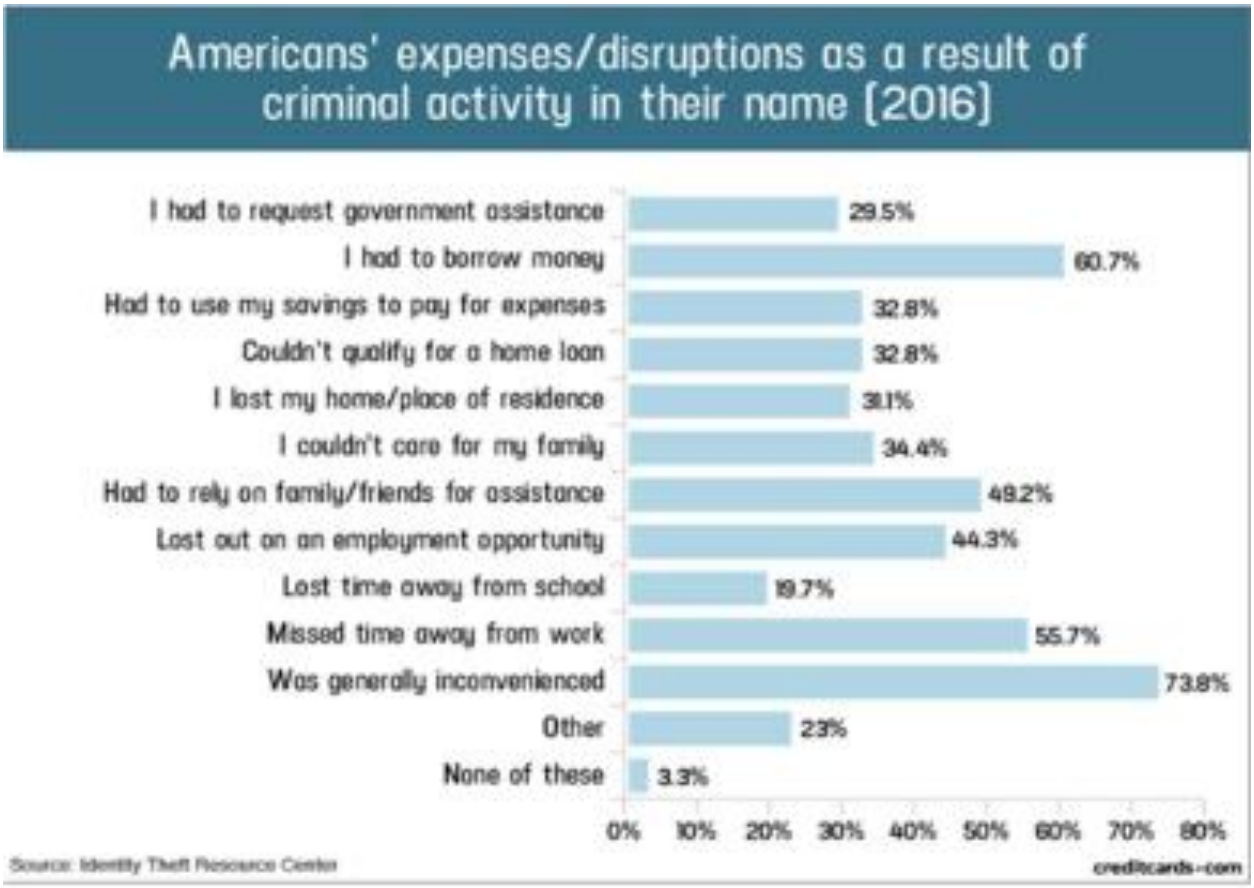
108. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

109. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[44]

110. It is within this context that Plaintiff and all other class members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

111. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

[43] Patrick Lucas Austin, 'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say, TIME (Aug. 5, 2019), accessible at https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last accessed on December 8, 2023).
[44] John W. Coffey, Difficulties in Determining Data Breach Impacts, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), accessible at http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf (last accessed on December 8, 2023).



112. Victims of the Data Breach, like Plaintiff and class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts of their privacy and credit because of the Data Breach.[45]

113. As a direct and proximate result of the Data Breach, Plaintiff and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and class members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their

[45] Guide for Assisting Identity Theft Victims, Federal Trade Commission, 4 (Sept. 2013), accessible at http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last accessed on December 8, 2023)..

financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other account information for unauthorized activity for years to come.

114. Plaintiff and class members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including Personal Information;

b. Improper disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Personal Information being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

e. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

115. Moreover, Plaintiff and class members have an interest in ensuring that their PII, which remains in the possession of Defendants, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiff's and class members' PII.

H. The Data Breach Was Foreseeable and Preventable

116. Data disclosures and data breaches are preventable.[46] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[47] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[48]

> "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[49]

117. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[50]

---

[46] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).
[47] Id. At 17.
[48] Id. at 28.
[49] Id.
[50] See How to Protect Your Networks from RANSOMWARE, at 3, FBI.gov, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed December 8, 2022).

118. Plaintiff and class members entrusted their PII to Defendants as a condition of receiving employment of other consumer goods and services. Plaintiff and class members understood and expected that Defendants or anyone in Defendants' position would safeguard their Personal Information against cyberattacks, delete or destroy PII that Defendants were no longer required to maintain, and timely and accurately notify them if their PII was compromised.

I. Plaintiff's and Class Members' Damages

119. To date, Defendants have done nothing to provide Plaintiff and class members with relief for the damages they have suffered because of the Data Breach. Zeroed-In only offered "Single Bureau Credit Monitoring" for a mere "twelve (12) months from the date of enrollment but did not disclose how it determined eligibility.[51] Not only did Defendants fail to provide adequate ongoing credit monitoring or identity protection services for individuals impacted by the Data Breach, but the credit monitoring identity theft protection services does nothing to compensate class members for damages incurred and time spent dealing with the Data Breach.

120. In fact, Plaintiff has spent time to conduct her own credit monitoring to determine whether her PII has been illegally because it is now on the Dark Web for cybercriminals to exploit, exchange, and sell. For example, Plaintiff put a freeze on her relevant accounts which were implicated due to the Data Breach. Additionally, Plaintiff scheduled an in-person meeting with her bank, which noticed suspicious activity on several "apps" as of late September and early October.

121. Ultimately, Plaintiff's self-efforts and Defendants' measly offer of credit-monitoring services are not able to contain the fallout resulting from the Data Breach. To date, Plaintiff continues to receive numerous notifications that her PII has been compromised on the Dark Web.

[51] See Notice of Data Event, n.1, supra.

122. Plaintiff and class members have been damaged by the compromise of their PII in the Data Breach.

123. As a direct and proximate result of Defendants' conduct, Plaintiff and class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and class members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

124. Plaintiff and class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and class members.

125. Plaintiff and class members have and will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Plaintiff and class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

127. Plaintiff and class members suffered actual injury from having their PII compromised

128. because of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their PII, a form of property that Zeroed-In obtained from Plaintiff and class members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

129. Further, because of Defendants' conduct, Plaintiff and class members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy with respect to that information.

130. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and class members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

a. 130.Moreover, Plaintiff and class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents

containing PII is not accessible online, is properly encrypted, and that access to such data is password protected.

131. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendants' failure to incur the costs necessary to implement adequate and reasonable cyber security training, procedures and protocols that were necessary to protect Plaintiff's and class members' PII.

132. Defendants maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

133. Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would result if Plaintiff's and class members' PII was stolen, including the significant costs that would be placed on Plaintiff and class members because of the breach.

134. The risk of improper disclosure of Plaintiff's and class members' PII was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure Plaintiff's and class members' PII from that risk left the PII in a dangerous condition.

135. Defendants disregarded the rights of Plaintiff and class members by, inter alia, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and class members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and class members prompt and accurate notice of the Data Breach.

CLASS ALLEGATIONS

136. Plaintiff brings this class action on behalf of herself and all members of the following Classes of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiff seeks certification of a Class defined as follows:

Nationwide Class

> All persons residing in the United States whose Personal Information was compromised in the Data Breach disclosed by Defendants on or about November 23, 2023, including all who were sent notice of the Data Breach.

137. Excluded from the class are Defendants and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

138. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

139. **Numerosity:** The members in the class are so numerous that joinder of all class members in a single proceeding would be impracticable. As noted above, Defendants reported that approximately 1.977 million individuals' information was exposed in the Data Breach.

140. **Commonality and Predominance:** Common questions of law and fact exist as to all class members and predominate over any potential questions affecting only individual class members. Such common questions of law or fact include, inter alia:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and class members' PII from unauthorized access and disclosure;

b. Whether Defendants' computer systems and data security practices used to protect Plaintiff's and class members' Personal Information violated the FTC Act and/or state laws and/or Defendants' other duties discussed herein;

c. Whether Zeroed-In failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and class members;

d. Whether Plaintiff and class members suffered injury as a proximate result of Defendants' negligent actions or failures to act;

e. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and class members' PII;

f. Whether an implied contract existed between class members and Defendants providing that Defendants would implement and maintain reasonable security measures to protect and secure class members' PII from unauthorized access and disclosure;

g. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and class members;

h. Whether Defendants' actions and inactions alleged herein constitute gross negligence;

i. Whether Defendants breached their duties to protect Plaintiff's and class members' PII; and

j. Whether Plaintiff and all other members of the class are entitled to damages and the measure of such damages and relief.

141. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

142. **Typicality:** Plaintiff's claims are typical of the claims of the class. Plaintiff, like all proposed members of the class, had her PII compromised in the Data Breach. Plaintiff and class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all class members.

143. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the class members. Plaintiff is an adequate representative of the class and has no interests adverse to, or conflict with, the class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

144. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for class members to individually seek redress from Defendants' wrongful conduct. Even if class members could afford individual litigation, the court system could not. Individualized litigation

creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On behalf of Plaintiff and the Class, as Against Both Defendants)

145. Defendants owed a duty to Plaintiff and all other class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

146. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and all other class members' PII and the importance of maintaining secure systems. Defendants knew, or should have known, of the many data breaches that targeted corporate entities in recent years.

147. Given the nature of Defendants' businesses, the sensitivity and value of the PII it maintains, and the resources at each of its disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

148. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and class members' PII.

149. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data

security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and class members' PII to unauthorized individuals.

150. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and class members, their PII would not have been compromised.

151. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
Negligence Per Se
(On behalf of Plaintiff and the Class, as Against Both Defendants)

152. Defendants' duties arise from, inter alia, from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

153. Plaintiff and class members are within the class of persons that Section 5 of the FTCA was intended to protect.

154. The harm occurring because of the Data Breach is the type of harm that Section 5 of the FTCA intended to guard against.

155. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and class members' PII to unauthorized individuals.

156. The injury and harm that Plaintiff and the other class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiff and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Class, as Against Both Defendants)

157. Plaintiff and class members either directly or indirectly gave Defendants their PII in confidence, believing that Defendants would protect that information. Plaintiff and class members would not have provided Defendants with this information had they known they would

not be adequately protected. Defendants' acceptance and storage of Plaintiff's and class members' PII created a fiduciary relationship between Defendants and Plaintiff and class members. In light of this relationship, Defendants must act primarily for the benefit of their employees and customers and other individuals who are otherwise affiliated or transacted with Defendants, which includes safeguarding and protecting Plaintiff's and class members' PII.

158. Defendants have a fiduciary duty to act for the benefit of Plaintiff and class members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and class members' PII, failing to comply with the data security guidelines and best practices, and otherwise failing to safeguard the PII of Plaintiff and class members it collected.

159. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class, as Against Defendant Dollar Tree)

160. Defendant Dollar Tree required Plaintiff and class members to provide, or authorize the transfer of, their PII for Defendants to provide services. In exchange, Defendant Dollar Tree entered implied contracts with Plaintiff and class members in which Defendant agreed to comply with their statutory and common law duties to protect Plaintiff's and class members' PII and to timely notify them in the event of a data breach.

161. Plaintiff and class members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

162. Plaintiff and class members fully performed their obligations under their implied contracts with Defendant.

163. Defendant breached its implied contracts by failing to safeguard Plaintiff's and class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

164. The losses and damages Plaintiff and class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and the class members.

COUNT V
Declaratory and Injunctive Relief
(On behalf of Plaintiff and the Class, as Against Both Defendants)

165. Defendants owe a duty of care to Plaintiff and class members that require them to adequately secure Plaintiff's and class members' PII.

166. Defendants still possess the PII of Plaintiff and the class members. Defendants has not satisfied their contractual obligations and legal duties to Plaintiff and the class members.

167. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and class members. Further, Plaintiff and class members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that led to such exposure.

168. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

169. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Personal Information not necessary for their provision of services;

e. Ordering that Defendants conduct regular database scanning and security checks; and

f. Ordering that Zeroed-In routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, patient personally identifiable information and patient protected health information.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully request that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: December 22, 2023

Respectfully submitted,

s/ Francesca Kester
Francesca Kester
FL Bar No. 1021991
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 Franklin Street
6th Floor
Tampa, Florida 33602
Phone: (813) 424-5618
Email: fkester@forthepeople.com

Jennifer S. Czeisler (*pro hac vice* to be filed)
STERLINGTON, PLLC
One World Trade Center
85th Floor
New York, New York 10007
Telephone: (212) 433-2993
jen.czeisler@sterlingtonlaw.com

Edward W. Ciolko (*pro hac vice* to be filed)
STERLINGTON, PLLC
One World Trade Center
85th Floor
New York, New York 10007
Telephone: (212) 433-2993
edward.ciolko@sterlingtonlaw.com

James M. Evangelista (*pro hac vice* to be filed)
EVANGELISTA WORLEY LLC
500 Sugar Mill Road

Suit 245A
Atlanta, GA 30350
Tel: (404) 205-8400
Fax: (404) 205-8395
jim@ewlawllc.com

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on December 22, 2023, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

s/ Francesca Kester